UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/650,105	08/29/2000	Baskaran Dharmarajan	MSFT115431	9027

26389 7590 10/27/2005

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/650,105	**Applicant(s)** DHARMARAJAN, BASKARAN	
	Examiner Taghi T. Arani	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 15 August 2005.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are presented for examination.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.1 14, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 8/15/2005 has been entered.

Response to Amendment

3. Applicant's amendment filed 8/15/2005 necessitated the new ground(s) of rejection presented in this Office action. Therefore, Applicant's arguments relating to the rejection of claims 1-21 are rendered moot.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 5, 8-9, 11, 13, 17, 19 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Kunzelman et al. (U.S. Patent 6,041,357 and Kunzelman hereinafter)

In regards to claim 1, Kunzelman teaches a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application that provides a different service than said second server-based application (Abstract, Fig. 1 and associated text, i.e. server A and Server B), comprising:

(a) receiving a request to access the service provided by said second server-based application wherein the service provided by said second server-based application is different than the service provided by said first server-based application (i.e. a migration of client from server A to server B) (col. 3, lines 34-44);

(b) in response to said request,

(i) determining a session length indicating a length of time said client computer has been authorized to access the service provided by said first server-based application (page 4, col. 40-59, Table 1, session token comprises time of session creation and Expiration (Time-to-live) of session);

(ii) calculating a hash value for an authorization ticket (col. 4, lines 28-38, i.e. server A verifies if the client is permitted to migrate and server A returns a session token, see also page 4, Table 1 shows session token elements wherein the session token is digitally signed (hash value is inherent in digital signature)) received from said first server-based application, said session length (Time of session creation and Expiration of session), and a secret shared between said client computer and said second server-based application (col. 5, lines 1-3, lines 33-37, i.e. a digitally signed session token using source server node's private key), and

(iii) transmitting a request for authorization to said second server-based application comprising said hash value and said authorization ticket (col. 5, lines 38-58, see also col. 6, lines 43-57).

In regards to claim 5, Kunzelman teaches that session data of the session token (an authorization ticket received from the first server-based application, the session length, and the secret shared key) is encrypted with the target server node's public key and digitally signed with the source server node's private key using a public key cryptosystem supplied by RSA data security (col. 7, lines 15-27). That is, calculating a hash value comprises performing an MD5 hash is inherent in RSA-signature with MD5 message digest as standard public key cryptosystem scheme.

In regards to claim 8, Kunzelman teaches that the first server-based application comprises an instant messaging server computer and that the second server-based application comprises a Web server computer (col. 1, lines 9-22, i.e. Kunzelman's servers are HTTP servers connected to the client)

In regards to claim 13, Kunzelman teaches a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application that provides a different service than said second server-based application (Abstract, Figure 1 and associated text, i.e. server A and Server B provide services to the client 12), comprising:

(a) receiving a request for authorization to access the service provided by said second server-based application from said client computer (col. 2, lines 29-54, see also col. 5, lines 3858, i.e. the client sends the session token to the target server (second server-based application)) comprising a hash value, an authorization ticket, and a session length (Fig. 3 and associated text, where the session token provided by the client comprises a digital signature (i.e. encrypted message digest (MD), Expiration of the session (i.e. a session length), see also col. 4, lines 28-

49) wherein the service provided by said second server-based application is different than the service provided by said first server-based application (col. 1, lines 5-8);

(b) computing a new hash value for said authorization ticket, said session length, and a copy of a secret shared between said client computer and said second server-based application (col.. 6, lines 43-57, i.e. the target server node decodes the session token, verifies its authenticity using public key cryptography. The Office infers that verification of the session token authenticity using public key inherently requires computing a new hash value for the session token, see also (col. 4, lines 28-38, wherein session token (page 4, Table 1) elements comprise Expiration of the session (i.e. session length) and that the session token is digitally signed (hash value is inherent in digital signature) using RSA public key cryptosystem (i.e. a shared secret between the client computer and the target sever node),

(c) determining whether said hash value received from said client computer is identical to said new hash value (col. 5, lines 38-58, see also col. 6, lines 43-57); and

(d) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application (col. 5, lines 40-42, i.e. server B processes session token, performing the necessary verification and decrypting of the session token and (col. 5, lines 63-col.6, line 11) that server B decides whether to accept the server migration request).

In regards to claims 9 and 17, the claim limitation recites a computer-controlled apparatus operative to perform the method of claims 1 and 13 respectively, therefore the same rejection applies.

In regards to claims 11 and 19, the claim limitation recites a computer-readable medium containing computer-readable instructions which, when executed by a computer, perform the method of Claims 1 and 13 respectively, therefore the same rejection applies.

In regards to claim 21, Kunzelman teaches that the first server-based application comprises an instant messaging server computer and that the second server-based application comprises a Web server computer (col. 1, lines 9-22, i.e. Kunzelman's servers are HTTP servers connected to the client).

5. **Claims 6-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzelman as applied to claim 1 above, in further view of Wang et al. (U.S. Patent 6,005,853 and Wang hereinafter).

In regards to claim 6, the system of Kunzelman teaches the system of claim 1 as discussed above.

The system of Kunzelman does not teach further comprising:

starting a persistence timer; determining whether the persistence timer has reached a predefined value prior to receiving a response from the second server-based application, and in response to determining that the persistence time has reached a predefined value prior to receiving a response from the second server-based application, deleting the authorization ticket, the session length and the hash value from the client computer.

Wang discloses a network access scheme (col. 3, lines 3-4).

Wang teaches that when a data packet (i.e. authentication ticket) is sent, a sequence variable is allocated and an acknowledgement timer (i.e. persistence timer) is set to prevent waiting indefinitely. When the acknowledgement timer times out and the number of retries has been exhausted, the machine deletes the sequence variable and returns to the idle state (col. 11, lines 6-50). The sequence variable of Wang is analogous to the authorization ticket, the session length and the hash value of the instant invention.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Wang to include starting a persistence timer; determining whether the persistence timer has reached a predefined value prior to receiving a response from the second server-based application; and in response to determining that the persistence time has reached a predefined value prior to receiving a response from the second server-based application, deleting the authorization ticket, the session length and the hash value from the client computer with the motivation to prevent waiting indefinitely (Wang, col. 11, lines 21-22).

In regards to claim 7, the system of Kunzelman does not teach that in response to determining that the persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving the response from the second server-based application and displaying the response at said client computer.

Wang teaches that in response to determining that the persistence timer has not reached a predefined value prior to receiving a response (i.e. acknowledgment package) from said second computer, receiving the response from the second server-based application and displaying the response (i.e. returning to the idle state) at said client computer (col. 11, lines 6-50)

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Wang to include that in response to determining that the persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving the response, from the second server-based application and displaying the response at said client computer with the motivation to prevent waiting indefinitely (Wang, col. 11, lines 21 22).

6. **Claims 2-4 , 10 and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzelman as applied to claim 1 above, in further view of Misra et al. (U.S. Patent 5,999,711 and Misra hereinafter) .

In regards to claim 2, While Kunzelman teaches Time of session creation and Expiration of the session (col. 4, Table 1), Kunzelman does not teach that the authorization ticket comprises a time stamp, and that determining a session length comprises subtracting said time stamp from an elapsed time counter to determine said session length.

Misra teaches that the authorization ticket comprises a time stamp (col. 7, lines 44-46). The Examiner takes Official Notice that computing a session length by subtracting a timestamp from an elapsed time counter is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Misra to include a timestamp within the authorization ticket and computing a session length by subtracting a timestamp from an elapsed time counter with the motivation to minimize the time period in which an eavesdropper may use a copied ticket (Misra, col. 7, lines 48-40).

In regards to claim 3, Kunzelman teaches that the elapsed time counter is started when said authorization ticket is received from said first computer (i.e. Time of session creation with Expiration of the session) (col. 4, Table 1, elements 3-4).

In regards to claim 4, Kunzelman teaches that the ticket is received from the first server-based application when the client computer is authorized to access the service provided by said first server-based application (col. 4, lines 4-10).

In regards to claim 10, the claim limitation recites a computer-controlled apparatus operative to perform the method of claim 2, therefore the same rejection applies.

In regards to claim 12, the claim limitation recites a computer-readable medium containing computer-readable instructions which, when executed by a computer, perform the method of Claim 2, therefore the same rejection applies.

7. **Claims 14-16, 18, 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzelman as applied to claim 13 above, in further view of Misra et al. (U.S. Patent 5,999,711 and Misra hereinafter) and Hershey et al. (U.S. Patent 5,481,539 and Hershey hereinafter).

In regards to claim 14, Kunzelman teaches the system of claim 13 as discussed above.

While Kunzelman teaches Time of session creation and Expiration of session (Time-to live), Kunzelman does not teach:

(e) in response to determining that the hash value received from the client computer is identical to the new hash value,

(i) determining whether a sum of the session length and a time stamp received as part of the authorization ticket is within a preset threshold value of a current time, and

(ii) in response to determining that the sum of the session length and the time stamp is within a preset threshold value, authorizing the client computer to access said second server-based application.

Misra teaches that the authorization ticket comprises a time stamp (col. 7, lines 44-46).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Misra to include a timestamp within the authorization ticket with the motivation to minimize the time period in which an eavesdropper may use a copied ticket (Misra, col. 7, lines 40-50).

Hershey discloses a system that relates to the field of digital message transmission (col. 1, lines 20-21).

Hershey teaches that a unit (i.e. client computer) will try to send a message packet (i.e. ticket) to a number of receivers (i.e. web servers) before the message expires, and that it determines whether a message expires by adding a "LIFETIME" (i.e. session length) value to a "TIMESTAMP" value in the message packet. This message is then compared to the current time to determine whether the message expired or not. If the message has not expired, then the message packet is rebroadcast and the remaining steps are performed (i.e. authorization continues as normal) (col. 7, lines 34-43)

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Hershey to include determining whether a sum of the session length and a time stamp received as part of the authorization ticket is within a preset threshold value of a current time and that in response to determining that the sum of the session length and the time stamp is within a preset threshold value, authorizing the client computer to access said second server-based application with the motivation to provide a highly fault tolerant method of relaying information to a desired communication unit (Hershey, col. 2, lines 53-54).

In regards to claim 15, Kunzelman teaches that in response to determining that the hash value received from the client computer is not identical to the new hash value, not authorizing said client computer to access said second server-based application (col. 5, line 66-col. 6, line 11).

In regards to claim 16, the system of Kunzelman does not teach that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value, it does not authorize the client computer to access the second server-based application.

Hershey teaches that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value (i.e. the message expired), it does not authorize the client computer to access the second server-based application (i.e. message packet is erased) (figure 5a, steps 57 and 49).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Kunzelman with the teachings of Hershey to include that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value, it does not authorize the client computer to access the second server-based application with the motivation to provide a highly fault tolerant method of relaying information to a desired communication unit (Hershey, col. 2, lines 53-54).

In regards to claim 18, the claim limitation recites a computer-controlled apparatus operative to perform the method of claim 14, therefore the same rejection applies.

In regards to claim 20, the claim limitation recites a computer-readable medium containing computer-readable instructions which, when executed by a computer, perform the method of Claim 14, therefore the same rejection applies.

Conclusion

8. Prior arts made of record, not relied upon:

U.S. Patent 6,877,095 to Allen.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. arani
Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
10/24/05